UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/875,095	06/07/2001	Kristofer Skantze	3782-0134P	7701

2292 7590 06/06/2006

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/875,095	SKANTZE, KRISTOFER	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5-14,16 and 18-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5-14,16 and 18-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 03/13/06 have been fully considered are persuasive. Due to applicant's arguments previous office action has been withdrawn and new grounds of rejection have been provided below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 5-6, 14, 18-19, 22, 27-30, and 32-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lapstun et al. (6,789,191) in view of Dorenbos (5,751,813) and further in view of Borgström (6,738,053 B1).

In reference to claims 1, 14, 27 and 35, Lapstun discloses a protocol for registering an interactive device with a registration server in a network connected to the interactive device and the registration server (column 2 lines 1-5). The system comprises obtaining, in the digital pen, a message in the form of a plurality of absolute position recorded from an absolute position coding pattern on a substrate (column 5 lines 1-3); obtaining, in the digital pen, at least one absolute position recorded from an absolute position coding pattern on a secure note (column 4 lines 46-52); sending said at least one absolute position recorded form the secure note to a database device (column 4 lines 55-60), in which said at least one absolute position is associated with an address of the receiving device (column 7 lines 49-58); receiving, in the digital pen, said address (column 17 lines 33-51) and an encryption key of

said receiving device, from the database device (column 32 lines 54-56); encrypting the message to be transmitted using said encryption key received from the database device (column 16 lines 14-16); obtaining a transmission channel form the digital pen to the receiving device (column 16 lines 14-16); transmitting the encrypted message to the receiving device (column 16 lines 14-16); and presenting the message to a receiver (column 6 lines 1-14).

Although Lapstun discloses encrypting the information at the pen, and it is inherent that for the receiving device to view the information it must be decrypted, Lapstun does not expressly disclose decrypting the received message.

Dorenbos a system and method for secure wireless transmission of information from a sender to a receiver, comprising: a sending device arranged for obtaining a message and a receiver identity (column 4 lines 43-47); encryption means for encrypting the message to be transmitted (Fig. 3 and column 5 lines 18-22); a transmission channel from the sending device (part 317 Fig. 3) to a receiving device for transmitting the encrypted information to the receiving device (column 5 lines 46-60); decryption means for decrypting the information in the receiving device (column 5 lines 47-48); display means for presenting the message to the receiver (part 127 Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to decrypt the information that has been encrypted as in Dorenbos in the system of Lapstun. One of ordinary skill in the art would have been motivated to do this because the information must be decrypted if it is to be understood by the user.

Although Lapstun suggests a form of displaying the received information (Fig 2), however Lapstun does not disclose the use of a secure note in which a pattern is connected to

a receiving device. Lapstun also does not discloses receiving an address of the receiving device from the database device.

Borgström discloses a method and system for initiating functions on an electronic device includes using a sensor to detect a pattern on a specially formatted surface wherein the pattern on the surface can be dots (abstract). The secure note disclosed by Borgström is the data surface (column 3 line 66 to column 4 line 11) is a piece of paper (column 4 line 30-31); and the pattern on the secure note is connected to a receiver; the receiver being processor or computer where the signal from the CCD is sent to a server (column 5 lines 18-42). Further more, although the system of Lapstun discloses the digital pen receiving an encryption key, Lapstun does not discloses receiving an address of the receiving device from the database device. Borgström discloses a system wherein the digital pen, when acting as an electronic pen client (column 9 lines 26-31), the electronic sends the address pattern to a name server that translates the detected position into a Uniform Resource Location (by definition an address) and then the name server sends it back to the electronic pen client (digital pen; Fig. 10A).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add to the functionality of the pen in Borgström to the pen in Lapstun so that Lapstun can utilize the address information shared in the system of Borgström. One of ordinary skill in the art would have been motivated to do this because it would enable it would increase the functionality of the pen by allowing the system to use certain address patterns can be associated with different functions or applications (Borgström column 2 line 39 to column 3 line 10).

In reference to claims 5, 18, 28 and 37, wherein the digital pen is arranged to encrypt the message in the sending device by a symmetric key and that the decryption means is

arranged to decrypt the message in the receiving device by the same key (column 32 lines 63-64).

In reference to claims 6, 19, 30 and 38, wherein the symmetric key has been agreed upon in advance and is stored in the digital pen and the receiving device (column 32 lines 36-39).

In reference to claim 22, further comprising a verification means for identification of a user to the digital pen: and/or identification of the receiver to the receiving device, said verification means being arranged to use identification measures, wherein the identification measures are at least on of a Pin-code, optical, sound, vibration, heat, speed, angle, times pressure, acceleration, absolute coordinate, handwritten signature, voice recognition, fingerprint sensor, or other biometric means (column 6 lines 30-40).

In reference to claims 29, 32, and 36, wherein the step of sending further comprises sending an identity of the pen to the database device (column 32 lines 19-35).

In reference to claim 33, further comprising displaying the address of the receiving device to a user of the digital pen and obtaining one of a confirmation and a rejection of the address from the user (column 32 lines 25-35).

In reference to claim 34, wherein at least one of the sending step, the receiving step and the transmitting step is carried out over the network (Fig. 2 in combination with column 32 lines 6-18).

In reference to claim 40, wherein sending said at least one absolute position recorded from the secure note to a database device occurs via Bluetooth through a mobile telecommunications device. The system of Lapstun discloses transmitting encrypted information wirelessly (column 16 lines 14-17) and therefore uses Bluetooth through a

mobile telecommunication device to send at least one absolute position recorded from the secure note.

In reference to claim 16 Lapstun does not disclose receiving address is obtained by transmitting said one position to a database, in which the absolute position code is associated with said one receiving address and using said receiving address for the transmission.

Borgström discloses a method and system for initiating functions on an electronic device includes using a sensor to detect a pattern on a specially formatted surface wherein the pattern on the surface can be dots (abstract). Borgström discloses transmitting said one position to a database on the server, in which the absolute position code is associated with said one receiving address (URL) and using said receiving address for the transmission (column 5).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add to the functionality of the pen in Borgström to the pen in Lapstun so that Lapstun can utilize the address information shared in the system of Borgström. One of ordinary skill in the art would have been motivated to do this because it would enable it would increase the functionality of the pen by allowing the system to use certain address patterns can be associated with different functions or applications (Borgström column 2 line 39 to column 3 line 10).

Claims 7-13, 20-21, 23-26, 31, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lapstun in view of Dorenbos and further in view of Borgström and further as applied to claims 5, 14, 18, and 27 above, and further in view of Schneier.

In reference to claims 7, 20, 31, Lapstun discloses, encrypting at least the symmetric key by a public key of an asymmetric key having a private key and public key and belonging

to the receiving device, decrypting the symmetric key by the private key of the receiving device; and using the symmetric key for decrypting the message during the key exchange (column 32 lines 1-56).

Schneier discloses the symmetric key is added to the message after encryption with the symmetric key; the encryption means is arranged to encrypt at least the symmetric key by a public key of an asymmetric key having a private key and a public key and belonging to the receiver; code is connected to at least one the decryption means is arranged to decrypt the symmetric key by the private key of the receiver in the receiving device; and the decryption means is arranged to use the symmetric key for decrypting the message (page 51 paragraph 1-2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a asymmetric key to encrypt a symmetric key and attach the key to the message as taught by Schneier in the system of Lapstun. One of ordinary skill in the art would have been motivated to do this because it is a common key-exchange protocol.

In reference to claims 8 and 21, wherein the encryption means is arranged to encrypt the already encrypted symmetric key in the sending device by a private key of an asymmetric key having a private key and a public key and belonging to the sender, the receiving device is arranged to obtain the sender public key, such as from the sending device or a separate server; and the decryption means is arranged to decrypt the symmetric key by the public key of the sender in the receiving device and by the private key of the receiver.

Lapstun does not disclose encrypt the already encrypted symmetric key in the sending device by a private key of an asymmetric key having a private key and a public key and belonging to the sender, the receiving device is arranged to obtain the sender public key, such as from the sending device or a separate server; and the decryption means is arranged to

decrypt the symmetric key by the public key of the sender in the receiving device and by the private key of the receiver.

Schneier teaches encrypt the symmetric key in the sending device by a private key of an asymmetric key having a private key and a public key and belonging to the sender, the receiving device is arranged to obtain the sender public key, such as from the sending device or a separate server; and the decryption means is arranged to decrypt the symmetric key by the public key of the sender in the receiving device and by the private key of the receiver (page 49). Schneier further teaches multiple encryption and therefore encrypting the already encrypted session key (page 367).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use multiple encryption algorithms on the same message as in Schneier in the system of Lapstun. One of ordinary skill in the art would have been motivated to do this because if one of the receipt of the message or the sender of the message does not trust the algorithm of the other party, with this method both algorithms may be used and the encryption will be as strong as the strongest algorithm.

In reference to claims 10, 23 and 39, further comprising encryption key generation means for obtaining a random seed for generating encryption key by means of the verification means during the identification step.

Although Lapstun disclose encrypting messages using keys, Lapstun does not disclose key generation means for obtaining a random seed for generating encryption key by means of the verification means during the identification step.

Schneier disclose the generation of random number for use as keys, which are used for identification as pass-phrases (page 423 and 173-174).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate random number keys as in Schneier in the system of Lapstun. One of ordinary skill in the art would have been motivated to do this because random bit strings provide good keys.

In reference to claims 11 and 24 further comprising: encryption key generation means for obtaining a random seed for generating an encryption key during the step of obtaining the message.

Lapstun does not disclose key generation means for obtaining a random seed for generating an encryption key during the step of obtaining the message.

Schneier discloses key generation means for obtaining a random seed for generating an encryption key during the step of obtaining the message (page 173).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate random number keys as in Schneier in the system of Lapstun. One of ordinary skill in the art would have been motivated to do this because random bit strings provide good keys.

In reference to claims 9, 12, and 25, wherein the sending device is arranged to generate a sender private key and sender public key pair, and is arranged to use a random seed obtained using a physical parameter of the sender, such as handwritten signature recognition, fingerprint information, or movement of the sending device or of the sending device, such as acceleration speed, time, vibration etc.

Lapstun does not disclose the sending device is arranged to generate a sender private key and sender public key pair, and is arranged to use a random seed obtained using a physical parameter of the sender, such as handwritten signature recognition, fingerprint

information, or movement of the sending device or of the sending device, such as acceleration speed, time, vibration etc.

However Schneier discloses a random seed obtained using a physical parameter (page 173).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate random number keys as in Schneier in the system of Lapstun. One of ordinary skill in the art would have been motivated to do this because random bit strings provide good keys.

In reference to claims 13 and 26 wherein the sender public key is added to the message, unencrypted, as sender identification.

Lapstun does not disclose the sender public key is added to the message, unencrypted, as sender identification.

Schneier discloses the key used as identification, pass-phrase, (page 174), further Schneier teaches a key added to the message (page 51).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to generate random number keys as in Schneier in the system of Lapstun. One of ordinary skill in the art would have been motivated to do this because random bit strings provide good keys.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HOSUK SONG
PRIMARY EXAMINER

PWK
Tuesday, May 30, 2006